Problem Set 1

- Due Date: **27 Sep, 2017**
- Turn in your problem sets electronically (LaTeX, pdf or text file) by email. If you submit handwritten solutions, start each problem on a fresh page.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Refering sources other than the text book and class notes is strongly discouraged. But if you do use an external source (eg., other text books, lecture notes, or any material available online), ACKNOWLEDGE all your sources (including collaborators) in your writeup. This will not affect your grades. However, not acknowledging will be treated as a serious case of academic dishonesty.
- The points for each problem are indicated on the side.
- Problems 1–4 are from O'Donnell's book and course.
- Be clear in your writing.

1. **[Fourier expansion]**

   Compute the Fourier expansions of the following functions. Please give some indication of how you arrived at the expansion; a bare formula does not suffice.

   (a) The *selection function* $\mathrm{Sel} : \{1,-1\}^3 \to \{-1,1\}$ which outputs x_2 if $x_1 = -1$ and outputs x_3 if $x_1 = 1$.

   (b) The indicator function $1_{\{a\}} : \{1,-1\}^n \to \{0,1\}$, where $a \in \{1,-1\}^n$.

   (c) The density function corresponding to the product probability distribution on $\{1,-1\}^n$ in which each coordinate has mean $\rho \in [-1,1]$;

   (d) The *inner product mod* 2 *function*, $\mathrm{IP}_{2n} : \mathbb{F}_2^{2n} \to \{-1,1\}$ defined by $\mathrm{IP}_{2n}(x_1,\ldots,x_n,y_1,\ldots,y_n) = (-1)^{x\cdot y}$. (Here $x \cdot y$ denotes the dot-product in the vector space $\mathbb{F}_2^n$.)

   (e) The *hemi-icosahedron function* (also called the *Kushilevitz function*), $\mathrm{HI} : \{1,-1\}^6 \to \{1,-1\}$, defined as follows: $\mathrm{HI}(x)$ is 1 if the number of 1's in x is 1, 2, or 6. $\mathrm{HI}(x)$ is -1 if the number of -1's in x is 1, 2, or 6. Otherwise, $\mathrm{HI}(x)$ is 1 if and only if one of the ten facets in the following diagram has all three of its vertices 1:

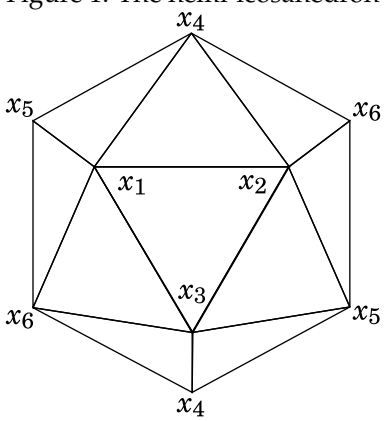
   (f) the *complete quadratic function* $\mathrm{CQ}_n : \mathbb{F}_2^n \to \{1,-1\}$ defined by $\mathrm{CQ}_n(x) = (-1)^{(\sum_{1\le i<j\le n} x_i x_j)}$.

   [Hint: Determine $\mathrm{CQ}_n(x)$ as a function of the number of 1s in the input modulo 4. You'll want to distinguish whether n is even or odd.]

2. **[Boolean dual and odd-even functions]**

   The *(boolean) dual* of $f : \{1,-1\}^n \to \mathbb{R}$ is the function $f^\dagger$ defined by $f^\dagger(x) = -f(-x)$. The function f is said to be *odd* if it equals its dual; equivalently, if $f(-x) = -f(x)$ for all x. The function f is said to be *even* if $f(-x) = f(x)$ for all x. Given any function $f : \{1,-1\}^n \to \mathbb{R}$, its *odd part* is the function $f^{\mathrm{odd}} : \{1,-1\}^n \to \mathbb{R}$ defined by $f^{\mathrm{odd}}(x) = (f(x) - f(-x))/2$, and its *even part* is the function $f^{\mathrm{even}} : \{1,-1\}^n \to \mathbb{R}$ defined by $f^{\mathrm{even}}(x) = (f(x) + f(-x))/2$.

Figure 1: The hemi-icosahedron



(a) Express $\widehat{f^\dagger}(S)$ in terms of $\widehat{f}(S)$.

(b) Verify that $f = f^{\text{odd}} + f^{\text{even}}$ and that f is odd (respectively, even) if and only if $f = f^{\text{odd}}$ (respectively, $f = f^{\text{even}}$).

(c) Show that

$$f^{\text{odd}} = \sum_{\substack{S \subseteq [n] \\ |S| \text{ odd}}} \widehat{f}(S)\,\chi_S, \qquad f^{\text{even}} = \sum_{\substack{S \subseteq [n] \\ |S| \text{ even}}} \widehat{f}(S)\,\chi_S.$$

3. **[Walsh–Hadamard matrices]**

A *Hadamard matrix* is any $N \times N$ real matrix with ± 1 entries and orthogonal rows. Particular examples are the *Walsh–Hadamard matrices* H_N, inductively defined for $N = 2^n$ as follows: $H_1 = \begin{bmatrix} 1 \end{bmatrix}$, $H_{2^{n+1}} = \begin{bmatrix} H_{2^n} & H_{2^n} \\ H_{2^n} & -H_{2^n} \end{bmatrix}$.

(a) Let's index the rows and columns of H_{2^n} by the integers $\{0, 1, 2, \ldots, 2^n - 1\}$ rather than $[2^n]$. Further, let's identify such an integer i with its binary expansion $(i_0, i_1, \ldots, i_{n-1}) \in \mathbb{F}_2^n$, where i_0 is the least significant bit and i_{n-1} the most. E.g., if $n = 3$, we identify the index $i = 6$ with $(0, 1, 1)$. Now show that the (γ, x) entry of H_{2^n} is $(-1)^{\langle \gamma, x \rangle}$.

(b) Show that if $f : \mathbb{F}_2^n \to \mathbb{R}$ is represented as a column vector in $\mathbb{R}^{2^n}$ (according to the indexing scheme from item 3a) then $2^{-n} H_{2^n} f = \widehat{f}$. Here we think of $\widehat{f}$ as also being a function $\mathbb{F}_2^n \to \mathbb{R}$, identifying subsets $S \subseteq \{0, 1, \ldots, n-1\}$ with their indicator vectors.

(c) Show that taking the Fourier transform is essentially an "involution": $\widehat{\widehat{f}} = 2^{-n} f$ (using the notations from item 3b).

(d) (Optional.) Show how to compute $H_{2^n} f$ using just $n 2^n$ additions and subtractions (rather than 2^{2n} additions and subtractions as the usual matrix-vector multiplication algorithm would require). This computation is called the *Fast Walsh–Hadamard Transform* and is the method of choice for computing the Fourier expansion of a generic function $f : \mathbb{F}_2^n \to \mathbb{R}$ when n is large.

4. (Sanders '06.) Let $A \subseteq \mathbb{F}_2^n$, let $\alpha = |A|/2^n$, and write $1_A : \mathbb{F}_2^n \to \{0, 1\}$ for the indicator function of A.

(a) Show that $\sum_{S \neq \emptyset} \widehat{1_A}(S)^2 = \alpha(1-\alpha)$.

(b) Define $A + A + A = \{x + y + z : x, y, z \in A\}$, where the addition is in $\mathbb{F}_2^n$. Show that either $A + A + A = \mathbb{F}_2^n$ or else there exists $S^* \neq \emptyset$ such that $|\widehat{1_A}(S^*)| \geq \frac{\alpha}{1-\alpha} \cdot \alpha$.

[Hint: if $A + A + A \neq \mathbb{F}_2^n$, show there exists $x \in \mathbb{F}_2^n$ such that $1_A * 1_A * 1_A(x) = 0$.]

5. **[linearity test of 3 functions]**

Consider the following modification of the BLR-linearity test towards testing linearity of 3 functions $f, g, h : \{0,1\}^n \to \{1,-1\}$ simultaneously.

BLR-3-Test^{f,g,h} : " 1. Choose $y, z \in_R \{0,1\}^n$ independently
2. Query $f(y), g(z),$ and $h(y+z)$
3. Accept if $f(y)g(z)h(y+z) = 1$. "

Clearly, if the three functions f, g, h are the same linear function, then the above test accepts with probability 1. Suppose one of the three functions f, g, h (say f) and its negation (i.e., $-f$) is δ-far from linear (this means $\max_\alpha |\widehat{f_\alpha}| \leq 1 - 2\delta$), show that

$$\Pr_{y,z}[\text{BLR-3-Test}^{f,g,h} \text{ rejects }] \geq \delta.$$

[Hint: The Cauchy-Schwarz inequality $(\sum a_i b_i)^2 \leq (\sum a_i^2) \cdot (\sum a_i^2)$ may come useful.]

6. **[recycling queries in linearity test]**

In lecture, we analyzed the soundness of the BLR-Test to show that if f is $(1/2 - \varepsilon)$-far from linear, then the test accepts with probability at most $1/2 + \varepsilon$. If we repeat this test k times, we obtain a linearity test which makes $3k$ queries and has the following property: if f is $(1/2 - \varepsilon)$-far from linear, then the test accepts with probability at most $(1/2 + \varepsilon)^k = 1/2^k + \delta$. Thus every additional 3 queries improves the soundness by a factor of $1/2$. In this problem, we show that this can be considerably improved.

Assume that both f and $-f$ are $(1-\varepsilon)/2$-far from linear (i.e., $\max_\alpha |\widehat{f_\alpha}| \leq \varepsilon$). Consider the following linearity test (parameterized by k).

Test$_k^f$: " 1. Choose $z_1, z_2, \ldots, z_k \in_R \{0,1\}^n$
2. For each distinct pair $(i,j) \in \{1, \ldots, k\}$
Check if $f(z_i)f(z_j)f(z_i + z_j) = 1$.
3. Accept if all the tests pass. "

Observe that this test makes at most $k + \binom{k}{2}$ queries. We will show below that the soundness of the test is roughly $2^{-\binom{k}{2}}$, thus showing that every additional query improves the soundness by a factor of $1/2$ (almost).

Assume that both f and $-f$ are $(1-\varepsilon)/2$-far from linear.

(a) Show that the acceptance probability of the above test is given by

$$\begin{aligned}\Pr[\text{acc}] &= \mathbb{E}_{z_1,\ldots,z_k}\left[\prod_{i,j}\left(\frac{1+f(z_i)f(z_j)f(z_i+z_j)}{2}\right)\right] \\ &= \frac{1}{2^{\binom{k}{2}}}\cdot\sum_{S\subseteq\binom{[k]}{2}}\mathbb{E}_{z_1,\ldots,z_k}\left[\prod_{(i,j)\in S} f(z_i)f(z_j)f(z_i+z_j)\right]\end{aligned}$$

(b) Consider any term in the above summation corresponding to a non-empty S (i.e., $\mathbb{E}_{z_1,\ldots,z_k}\left[\prod_{(i,j)\in S} f(z_i)f(z_j)f(z_i+z_j)\right]$). Suppose $(1,2)\in S$. Show that

$$\mathbb{E}_{z_1,\ldots,z_k}\left[\prod_{(i,j)\in S} f(z_i)f(z_j)f(z_i+z_j)\right] \le \mathbb{E}_{z_1,z_2}[f(z_1+z_2)g(z_1)h(z_2)]$$

for some functions $g,h:\{1,-1\}^n\to\{\pm 1\}$.

[Hint: Fix all the variables other than z_1 and z_2 such that that the expectation is maximized.]

(c) Use the result of item 5 to conclude that the expression in the above (for non-empty sums) is at most ε (i.e., $\mathbb{E}_{z_1,\ldots,z_k}\left[\prod_{(i,j)\in S} f(z_i)f(z_j)f(z_i+z_j)\right]\le\varepsilon$ for non-empty S).

(d) Conclude that $\Pr[\text{acc}]$ is at most $2^{-\binom{k}{2}}+\varepsilon$.

7. **[derandomized linearity testing]**

A subset $S\subseteq\{0,1\}^n$ is said to be an ε-biased set if for all $\alpha\in\{0,1\}^n\setminus\{0^n\}$, we have $|\Pr_{x\in S}[\langle x,\alpha\rangle=1]-\Pr_{x\in S}[\langle x,\alpha\rangle=0]|\le\varepsilon$.

Consider the following modification of the BLR test to check if $f:\{0,1\}^n\to\{\pm1\}$ is linear:

S-derandomized BLR-Test^f : " 1. Choose $y\in_R\{1,-1\}^n$ and $z\in_R S$ independently
2. Query $f(y), f(z)$, and $f(y+z)$
3. Accept if $f(y)f(z)f(y+z)=1$. "

Observe that the number of random coins required for this test is only $n+\log_2|S|$. There exist explicit constructions of ε-biased sets S of size at most $O(n^2/\varepsilon^2)$. Thus, the randomness is at most $n+O(\log n+\log(1/\varepsilon))$ as opposed to $2n$ for the (non derandomized) BLR test. In this problem, we will show that this S-derandomized test performs as well as the BLR test in terms of soundness. More precisely, we will show that $\Pr[\text{acc}]\ge(1+\delta)/2$, then there exists a Fourier coefficient of absolute value at least $\sqrt{\delta^2-\varepsilon}$, thus matching the soundness of the BLR test but for the ε loss factor.

(a) Show that if S is an ε-biased set then $|\mathbb{E}_{x\in S}[\chi_\alpha(x)]|\le\varepsilon$ forall $\alpha\neq 0^n$.

(b) Show that if f is a linear function (i.e, $f=\chi_\beta$), f passes the S-derandomized BLR-Test with probability 1.

For two functions $f,g:\{0,1\}^n\to\mathbb{R}$, define the inner product $\langle f,g\rangle_S$ and S-norm $\|f\|_S$ as

follows:

$$\langle f, g \rangle_S = \mathbb{E}_{z \in S} [f(z)g(z)]; \qquad \|f\|_S = \sqrt{\langle f, f \rangle_S}.$$

(c) For an arbitrary $f : \{0,1\}^n \to \{\pm 1\}$, show that the acceptance probability of the above test is given by

$$\begin{aligned} \Pr[\text{acc}] &= \frac{1}{2}\left(1 + \sum_\alpha \widehat{f_\alpha}^2 \cdot \langle f, \chi_\alpha \rangle_S\right) \\ &= \frac{1}{2}\left(1 + \left\langle f, \sum_\alpha \widehat{f_\alpha}^2 \chi_\alpha \right\rangle_S\right). \end{aligned}$$

(d) Use the fact that S is an ε-biased set and f is a $\{\pm 1\}$-valued function to prove that

$$\left|\left\langle f, \sum_\alpha \widehat{f_\alpha}^2 \chi_\alpha \right\rangle_S\right| \leq \sqrt{(1-\varepsilon)\sum_\alpha \widehat{f_\alpha}^4 + \varepsilon}.$$

(e) Conclude that if the S-derandomized BLR-Test accepts with probability at least $(1+\delta)/2$, then there exists an α such that $|\widehat{f_\alpha}| \geq \sqrt{\delta^2 - \varepsilon}$.